2/23/11

Problems on Index and Normal subgroups

1) Recall $Aut(G) = \{\varphi \mid \varphi : G \to G, \varphi \text{ is an isomorphism}\}$
Define for $g, h \in G$, $\varphi_h(g) = hgh^{-1}$
(Check that φ_h is an automorphism)
The <u>inner</u> automorphisms are:
$Inn(G) = \{\varphi_h : h \in G\}$
Show $Inn(G) \trianglelefteq Aut(G)$

2) Let $H_n = \{kn \mid k \in \mathbb{Z}\}$ for some $n \in \mathbb{N}$
$H_n \leq \mathbb{Z}$, Compute $[\mathbb{Z} : H_n]$

3) Determine $Aut(\mathbb{Z})$

1) Check φ is an automorphism
$\varphi_h : G \to G$, $\varphi_h(g) = hgh^{-1}$ $(h \in G)$
Check that φ_h is bijective & a homomorphism.
<u>φ_h injective</u>
Suppose $g, k \in G$ and $\varphi_h(g) = \varphi_h(k)$
then $hgh^{-1} = hkh^{-1}$
multiply on the left by h^{-1} and on the right by h to get $g = k$
<u>φ_h surjective</u>
set $k = h^{-1}gh$ for $g \in G$.
Then $\varphi_h(k) = hkh^{-1} = h(h^{-1}gh)h^{-1} = g$
<u>φ_h is a homomorphism</u>
let $k, g \in G$ $\varphi_h(g)\varphi_h(k) = (hgh^{-1})(hkh^{-1})$
$= hgkh^{-1} = \varphi_h(gk)$
$\therefore \varphi_h$ is an isomorphism.

Now show $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$

Check first that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$

Verify, $\forall\, h, k \in G$:

- $\varphi_h \varphi_k \in \mathrm{Inn}(G)$
- $(\varphi_h)^{-1} \in \mathrm{Inn}(G)$

(two-step subgroup test)

$$
\begin{aligned}
- \varphi_h \varphi_k (g) &= \varphi_h(\varphi_k(g)) \\
&= \varphi_h(kgk^{-1}) \\
&= hkgk^{-1}h^{-1} \\
&= (hk)\, g\, (kh)^{-1} \\
&= \varphi_{hk}(g)
\end{aligned}
$$

So, $\varphi_h \varphi_k = \varphi_{hk} \in \mathrm{Inn}(G)$

$- (\varphi_h)^{-1} \in \mathrm{Inn}(G)$

observe that
$$
\begin{aligned}
\varphi_h \varphi_{h^{-1}}(g) &= \varphi_h(\varphi_{h^{-1}}(g)) \\
&= \varphi_h(h^{-1}gh) \\
&= hh^{-1}ghh^{-1} = g
\end{aligned}
$$

similarly, $\varphi_{h^{-1}} \varphi_h(g) = g$ also.

Since the identity of $\mathrm{Aut}(G)$ is the map $\varphi_{e_G}(g) = g$, this shows that

$\varphi_h \varphi_{h^{-1}} = \varphi_{h^-} \varphi_h = \varphi_{e_G}$

Hence, $(\varphi_{h^{-1}}) = \varphi_{h^{-1}} \in \mathrm{Inn}(G)$

This shows $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Show $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$

i.e. show $\forall\, \varphi \in \mathrm{Aut}(G)$, $\varphi\, \mathrm{Inn}(G)\, \varphi^{-1} = \mathrm{Inn}(G)$

let $h, g \in G$.
$$
\begin{aligned}
&\varphi \varphi_h \varphi^{-1}(g) \\
&= \varphi(\varphi_h(\varphi^{-1}(g))) \\
&= \varphi(h\, \varphi^{-1}(g)\, h^{-1}) \\
&= \varphi(h)\, \varphi(\varphi^{-1}(g))\, \varphi(h^{-1}) \\
&\qquad \text{(since } \varphi \text{ is a homomorphism)} \\
&= \varphi(h)\, g\, \varphi(h^{-1}) \\
&= \varphi(h)\, g\, \varphi(h)^{-1} = \varphi_{\varphi(h)}(g)
\end{aligned}
$$

$\Rightarrow \varphi \varphi_h \varphi^{-1} \in \mathrm{Inn}(G)$ ($\varphi \varphi_h \varphi^{-1} = \varphi_{\varphi(h)}$

This shows $\varphi\, \mathrm{Inn}(G)\, \varphi^{-1} \subseteq \mathrm{Inn}(G)$. reverse similar. $\therefore \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$

2) $H_n \leq \mathbb{Z}$, $H_n = \{k \cdot n : k \in \mathbb{Z}\}$ $n \in \mathbb{N}$
calculate $[\mathbb{Z} : H_n]$ = # of distinct left cosets
When, for $s, t \in \mathbb{Z}$, do we have
$sH_n = tH_n$?
We know either $sH_n \cap tH_n = \emptyset$ or
$sH_n = tH_n$.
We know that $s \in s+H_n$ since $0 \in H_n$.
when is $s \in t+H_n$?
$s \in t+H_n$ if there is a k with $s = t+kn$
Hence, we must have that s and t are
congruent modulo n.
If s and t are not congruent modulo n,
then $s \neq t+kn$ for some $k \in \mathbb{Z}$
The list of cosets is then,
H_n, $1+H_n$, $2+H_n$, ..., $(n-1)+H_n$
[$n+H_n = H_n$ since $n \cong$ to zero modulo n]
There are n distinct left cosets since $|\mathbb{Z}_n| = n$
Hence, $[\mathbb{Z} : H_n] = n$

[<u>Note</u>: $[\mathbb{Z} : \{0\}] = \infty$]

3) Determine $Aut(\mathbb{Z})$
- First determine $Inn(\mathbb{Z}) = \{\varphi_n : n \in \mathbb{Z}\}$
$\varphi_n(k) = n + k - n = k$
$\varphi_n = \varphi_0 \ \forall n \in \mathbb{Z}$, hence $Inn(\mathbb{Z})$ is the
trivial group with one element
- try $\psi_n(k) = nk$ then $\psi_n(0) = 0$, $\psi_n(1) = n$,
$\psi_n(-1) = -n$, $\psi_n(2) = 2n$ ... Doesn't
work since you only get multiples of $n \Rightarrow \psi$ not biject.
This example shows that we must have $|\varphi(1)| = 1$
for any automorphism φ (φ is determined by
$\varphi(1)$ since $\mathbb{Z}$ is cyclic with generator 1)
we can have $\varphi(1) = -1$ or $\varphi(1) = 1$
$Aut(\mathbb{Z}) \cong \mathbb{Z}_2$

More on Group Theory

3/7/11

Normal subgroups and decomposition of groups
Chap 15 → 16

Idea: let V be a finite dimensional vector space ($V = \mathbb{R}^n$). Let $W \subseteq V$ be a vector space of V ($W = \mathbb{R}^m$, $m < n$)
Then $\exists$ a subspace $U \subseteq V$ with
$U \cap W = \{0\}$ and V is isomorphic to
$U \oplus W$ (as a vectorspace) ($U = \mathbb{R}^{n-m}$)
V "=" $U \oplus W$, U "=" V/W

What about for groups?
Let G be a (finite) group, Let $H \leq G$.
Does there exist $K \leq G$ with
$H \cap K = \{e_G\}$ and $G \cong H \times K$?
In some sense, K "=" G/H
If you consider $H \times \{e_K\} \leq H \times K$
$H \times \{e_K\} \cong H$ and $H \times \{e_K\} \trianglelefteq H \times K$
(proved before break)
This suggests that for a decomposition
$G \cong H \times K$ to exist, we need $H \trianglelefteq G$
Recall that we wanted also K "=" G/H.
If G is finite and $G \cong H \times K$ then
$|G| = |H| \cdot |K| \Rightarrow \frac{|G|}{|H|} = |K|$
Recall $\frac{|G|}{|H|} = [G:H]$, the number of left cosets of H in G.
This suggests that $\exists$ a group structure on the left cosets of H in G.

→

Suppose $H \trianglelefteq G$, Let $g, k \in G$.
$(gH) * (kH) = (gk)H$.
↑ this defines a binary operation on the left cosets of H in G

To get a group out of this, we need to check:
1) associativity
2) identity
3) inverse
4) is the operation "$*$" well-defined.

Worrying about (4):
The problem is that we can write
$gH = g_1H$ for $g \neq g_1$ and $kH = k_1H$ for $k \neq k_1$
we must check that $(gH) * (kH) = (g_1H) * (k_1H)$
we need:

<u>Lemma</u>: $gH = kH$ iff $g^{-1}k \in H$
<u>Pf</u>: $\Rightarrow$ Suppose $gH = kH$. $g \in gH$. Since $gH = kH$, $g \in kH$, so $\exists$ an $h \in H$ with $g = kh$. Then multiplying on the left by k^{-1}, $k^{-1}g = h \in H$. Then $g^{-1}k = (k^{-1}g)^{-1} = h^{-1} \in H$.
$\Leftarrow$ Suppose $g^{-1}k \in H$ then $\exists$ $h \in H$ with $g^{-1}k = h$. Multiplying on the left by g we have $k = gh$. This implies $k \in kH \cap gH$. This shows $kH \cap gH \neq \emptyset$, so $kH = gH$. ∎

Thm: let $H \trianglelefteq G$. Then the operation "$*$" on the left cosets of H in G given by $(g, k \in G)$, $(gH) * (kH) = (gk)H$ yields a group structure on the left cosets.

Pf: 1) associativity

let $g, k, t \in G$. $(gH * kH) * tH$

$= ((gk)H) * (tH) = (gkt)H$ — since multiplication on G is associative

$= (g(kt))H = gH * (kt)H$

$= gH * (kH * tH)$ ✓

2) Identity

$e_G H = H$.

If $g \in G$, $(gH) * (e_G H) = (g e_G) H = gH$

$= (e_G g) H = (e_G H) * (gH)$

3) Inverse

If $g \in G$, $(gH)^{-1} = g^{-1} H$

check: $gH * g^{-1}H = (gg^{-1})H = e_G H$

and $g^{-1}H * gH = (g^{-1}g)H = e_G H$ $= $ ✓

4) "$*$" is well defined

Suppose $g, g_1, k, k_1 \in G$ and

$gH = g_1 H$, $kH = k_1 H$

Check that $\underset{(gk)H}{\underset{\|}{gH * kH}} = \underset{(g_1 k_1)H}{\underset{\|}{g_1 H * k_1 H}}$.

By lemma, we need only show $(gk^{-1})(g_1 k_1) \in H$. Since $gH = g_1 H$, $kH = k_1 H$, $\exists$ $h, h' \in H$ with $g = g_1 h$, $k = k_1 h'$.

$(gk)^{-1}(g_1 k_1) = k^{-1} g^{-1} g_1 k_1 = (k_1 h')^{-1} (g_1 h)^{-1} g_1 h_1$

$= (h')^{-1} k_1^{-1} h^{-1} \cancel{g_1^{-1} g_1} k_1 = (h')^{-1} k_1^{-1} h^{-1} k_1$.

Since $H \trianglelefteq G$, $k_1^{-1} H k_1 = H$. Then $\exists$ an $h'' \in H$ with $k_1^{-1} h k_1 = h''$. Hence, $(gk)^{-1}(g_1 k_1)$

$= (h')^{-1} k_1^{-1} h^{-1} k_1 = (h')^{-1} h'' \in H$. By lemma $gkH = g_1 k_1 H$ ∎